Claims

1. A method for the secure transmission of data from a distributor to a client over a computer network, the method comprising:
   (a) encrypting the data using an encryption confidentiality key known to the client but not the distributor;
   (b) storing the encrypted data at the distributor;
   (c) generating a message by further encrypting the encrypted data using an encryption transmission key, the corresponding transmission decryption key being known to the client; and
   (d) transmitting the message to the client.

2. A method as claimed in claim 1 in which, on receipt of the message, the client confirms the integrity of the transmission by decrypting the message using the transmission key.

3. A method as claimed in claim 2 in which the client confirms the confidentiality of the data by decrypting the encrypted data using a confidentiality decryption key corresponding to the confidentiality encryption key.

4. A method as claimed in any one of claims 1 to 3 in which the data comprises or includes a cryptographic key.

5. A method as claimed in any one of claims 1 to 3 in which the data comprises or includes a program.

6. A method as claimed in any one of claims 1 to 3 in which the data comprises or includes licence or configuration information.

7. A method as claimed in any one of claims 1 to 4 in which the distributor provides key management functions, for example key generation, for the client.

8. A method as claimed in any one of claims 1 to 4 in which the client is adapted to use cryptographic keys but not to generate them, instead requesting a key from the distributor as required

9. A method as claimed in any one of the preceding claims in which the distributor comprises a repository in communication with a plurality of providers, each provider being responsible for sending messages to one of a plurality of clients.

10. A method as claimed in any one of claims 1 to 9 in which the encrypted data is stored in a non-secure part of the repository.

11. A method as claimed in any one of claims 1 to 9 in which the providers include respective insecure computers which relay to the users messages generated by the repository.

12. A method as claimed in any one of claims 1 to 9 in which the providers include respective secure computers.

13. A method as claimed in any one of claims 1 to 12 in which each secure computer within a provider generates messages using a cryptographic key obtained from the repository.

14. A method as claimed in claim 9 in which encrypted data held within the repository is divided into data sets, each data set being associated with a respective policy which defines how the data within the data set may be used.

15. A method as claimed in claim 14 in which data from a particular data set, when sent by the provider, is accompanied by the respective policy.

16. A method as claimed in claim 15 in which the policy is run by the provider.

17. A method as claimed in claim 14 or 15 in which the policy is run by the client.

18. A method as claimed in claim 14 in which the policy is run by the repository

19. A method as claimed in claim 9 in which a plurality of regions are defined within the repository, each region containing information on the secure computers that are permitted to make requests for or otherwise manipulate data held by the repository.

20. A method as claimed in claim 9 in which the said secure computers include that of the provider.

21. A method as claimed in claim 9 in which the said secure computers include those of the clients.

22. A method as claimed in claim 19 when dependent upon claim 14 in which each region further includes a plurality of data sets.

23. A method as claimed in claim 19 when dependent upon claim 14 in which each region is associated with a respective region policy which defines how the information within the region may be used.

24. A method as claimed in claim 19 when dependent upon claim 14 in which each region further contains one or more authority groups, the or each group defining a set of secure computers that are permitted to carry out certain tasks.

25. A method as claimed in claim 24 in which a given secure computer may belong to a plurality of authority groups.

26. A method as claimed in claim 24 in which each region includes a region authority group which is responsible for administrative functions relating to its respective region.

27. A method as claimed in claim 26 in which the region authority group is responsible for revoking a secure computer from a region.

28. A method as claimed in claim 24 in which the information within the or each authority group is encrypted and is confidential from the repository.

29. A method as claimed in claim 19 in which the information within the or each authority group is encrypted and is confidential from the provider.

30. A method as claimed in claim 19 in which the information within each authority group, when there is more than one such group, is encrypted and is confidential from other groups.

31. A computer security module having means for receiving from a sender a message comprising twice-encrypted data, means for confirming the integrity of the message by decrypting it according to a protocol known to both the module and the sender, and means for confirming that the confidentiality of the data has been preserved by further decrypting the decrypted message using a secret known to the module but not to the sender.

32. A computer system including a plurality of clients, each having a security module as claimed in claim 31, and a provider arranged to send messages, as required, to the said clients.

33. A computer system as claimed in claim 32 in which the provider includes a secure computer.

34. A computer system as claimed in claim 33 in which the secure computer within the provider includes a security module as claimed in claim 31.

35. A computer system as claimed in any one of claims 32 to 34 including a plurality of providers, and a repository arranged to send data, as required, to the said providers.

36. A computer system as claimed in claim 32 in which encrypted data is stored at the provider, and is re-encrypted prior to being sent as a message to the client.

37. A computer system as claimed in claim 35 in which encrypted data is stored at the repository, and is re-encrypted prior to being sent as messages to the providers.

38. A computer system as claimed in any one of claims 31 to 37 in which encrypted data is stored in a non-secure part of the repository.

39. A computer system as claimed in claim 35 in which the providers comprise respective insecure computers which relay to the users messages generated by the repository.

40. A computer system as claimed in claim 35 in which encrypted data held within the repository is divided into data sets, each data set being associated with a respective policy which defines how the data within the data set may be used.

41. A computer system as claimed in claim 40 in which data from a particular data set, when sent by the provider, is accompanied by the respective policy.

42. A computer system as claimed in claim 41 in which the policy is run by the provider.

43. A computer system as claimed in claim 41 or 42 in which the policy is run by the client.

44. A computer system as claimed in claim 40 in which the policy is run by the repository.

45. A computer system as claimed in claim 35 in which a plurality of regions are defined with the repository, each region containing information on the secure computers that are permitted to make requests for or otherwise manipulate data held by the repository.

46. A computer system as claimed in claim 45 when dependent upon claim 33 in which the said secure computers include that of the provider.

47. A computer system as claimed in claim 45 when dependent on claim 2 in which the said secure computers include those of the clients.

48. A computer system as claimed in claim 45 when dependent upon claim 40 in which each region further includes a plurality of data sets.

49. A computer system as claimed in claim 45 in which each region is associated with a respective region policy which defines how the information within the region may be used.

50. A computer system as claimed in claim 45 in which each region further contains one or more authority groups, the or each group defining a set of secure computers that are permitted to carry out certain tasks.

51. A computer system as claimed in claim 50 in which a given secure computer may belong to a plurality of authority groups.

52. A computer system as claimed in claim 50 in which each region includes a region authority group which is responsible for administrative functions relating to its respective region.

53. A computer system as claimed in claim 52 in which the region authority group is responsible for revoking a secure computer from a region.

54. A computer system as claimed in claim 50 in which the information within the or each authority group is encrypted and is confidential from the repository.

55. A computer system as claimed in claim 50 in which the information within the or each authority group is encrypted and is confidential from the provider.

56. A computer system as claimed in claim 50 in which the information within each authority group, when there is more than one such group, is encrypted and is confidential from the other group.

57. A method for the secure transmission of data to a client, over a computer network, the method comprising:

(a) providing, at a remote data distributor, encrypted data the decryption of which requires knowledge of a secret known to the client;

(b) opening a secure channel between the distributor and the client, the channel defining a cryptographic protocol agreed by both the distributor and client;

(c) at the distributor, further encrypting the encrypted data according to the protocol to generate a secure message, and transmitting the message to the client; and

(d) at the client:

(i) confirming the integrity of the transmission by decrypting the message according to the protocol; and

(ii) recovering the data by decrypting the encrypted data using the secret.

58. A method as claimed in claim 57 in which the data comprises or includes a cryptographic key.

59. A method as claimed in claim 58 in which the distributor provides key management functions, for example key generation, for the client.

60. A method as claimed in claim 58 in which the client is adapted to use cryptographic keys but not to generate them, instead requesting a key from the distributor as required.

61. A method as claimed in claim 58 in which the key is used in a secure process by the client.

62. A method as claimed in claim 57 in which the data comprises or includes a program.

63. A method as claimed in claim 57 in which the data comprises or includes licence or configuration information.

64. A method as claimed in any one of claims 57 to 63 in which the secret known to the client is not known to the distributor.

65. A method as claimed in claim 64 in which the distributor generates the message by calculating

encrypt(wrap({Ke-decrypt}, Kw-wrap), Ks)

where:

(i) wrap (a,b) denotes 'wrap key a with key b',

(ii) Ke-decrypt is the decryption key corresponding to an encryption key Ke-encrypt with which the data was encrypted,

(iii) Ks is a session key generated according to the said protocol, and

(iv) Kw-wrap is a wrapping key.

66. A method as claimed in claim 64 in which the distributor generates the message by calculating

Encrypt (B,Ks)

Where B has been received by the distributor in advance by some secure process, B being defined by wrap({Ke-decrypt}, Kw—wrap)

Where:

(i) wrap (a,b) denotes 'wrap key a with key b',

(ii) Ke-decrypt is the decryption key corresponding to an encryption key Ke-encrypt with which the data was encrypted,

(iii) Ks is a session key generated according to the said protocol, and

(iv) Kw-wrap is a wrapping key.

67. A method as claimed in claim 65 or 66 in which the client has a symmetric entity confidentiality key, Kec-secret, which has been securely transferred in advance to the distributor, the distributor then using Kec-secret as Kw-wrap.

68. A method as claimed in claim 65 or claim 66 in which the client has an asymmetric entity confidentiality key pair, Kec-public/Kec-private, Kec-public having been securely transferred in advance to the distributor, the distributor then using Kec-public as Kw-wrap.

69. A method as claimed in claim 64 in which the message generation includes wrapping the encrypted data with a symmetric entity confidentiality key which has been securely transferred in advance to the distributor.

70. A method as claimed in claim 64 in which the message generation includes wrapping the encrypted data with the public part of an asymmetric entity confidentiality key pair, the said public part having been securely transferred in advance to the distributor.

71. A method as claimed in claim 69 in which the distributor holds the said public part of the key pair confidential.